San Mateo County
Community College District

Internal Control Plan

Draft

July 30, 2025

SAN MATEO COUNTY
COMMUNITY
COLLEGE DISTRICT

Cañada College • College of San Mateo • Skyline College

LETTER FROM THE CHANCELLOR | 2025-2026: THE YEAR OF ACCOUNTABILITY

July 30, 2025

Dear District Community:

At SMCCCD, our commitment to transparency, accountability, operational excellence, and efficiency is a major priority for the next few years, with the adoption by our Board of Trustees of our Performance Audit Unit. I am proud to present the first draft of our 2025 Internal Control Plan (ICP).

This plan is bold and aspirational, and reflects our dedication to sound governance, risk management, and compliance within applicable laws and regulations. By adhering to the principles outlined in this document, we are setting the community college district standard statewide, as we aim to safeguard our resources, uphold our values, and support our mission of transforming lives through education. By doing so, we also engender deeper confidence in our operations, data integrity, and as stewards of the public trust.

Our draft ICP has been developed because Staff, alongside our Board of Trustees, adopted a major focus on transparency and accountability. The ICP also reflects the recommendations that came from the 2024 San Mateo County Civil Grand Jury Report on Internal Controls – recommending that all public entities in the County adopt a system of internal controls, and further recommended a system based on the Federal Government's standard of internal control: *The Green Book*. The Green Book itself draws from input from individuals knowledgeable about internal control, drawn from federal, state, and local government; the private sector; and academia. This draft ICP also incorporates best practices adapted from leading public and private educational institutions. It is the district's intent that this Plan serves as a living document, regularly reviewed and updated to meet the evolving needs of our district and the communities we serve.

I encourage all members of the district and our community to engage with this plan and provide feedback. It is our hope that this document will help us all contribute to a culture of excellence, integrity, and accountability.

Sincerely,

Melissa

Melissa Moreno, J.D., Chancellor
San Mateo County Community College District

SAN MATEO COUNTY COMMUNITY COLLEGE DISTRICT
DRAFT **INTERNAL CONTROL PLAN**

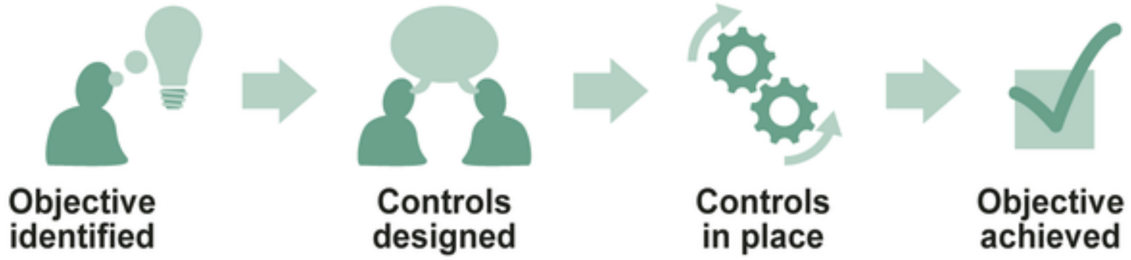
INTRODUCTION

San Mateo County Community College District (SMCCCD or "the District") is committed to maintaining a robust internal control system to ensure the effectiveness and efficiency of operations, the reliability of financial and non-financial reporting, and compliance with applicable laws and regulations. This plan incorporates elements from the Federal Government's Green Book.

Effective internal control is vital for SMCCCD to achieve its mission and objectives. Internal control is broadly defined as "a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved".

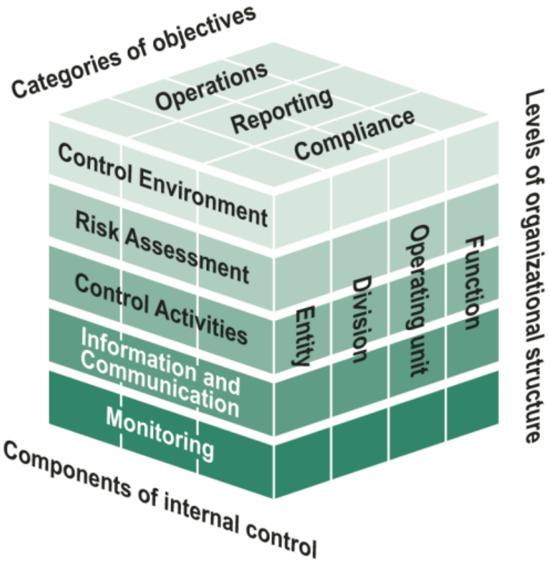
These objectives typically fall into three categories:

- Operations - efficient and effective operations
- Reporting - reliable internal and external reports
- Compliance - adherence to laws and regulations



Source: GAO. | GAO-14-704G

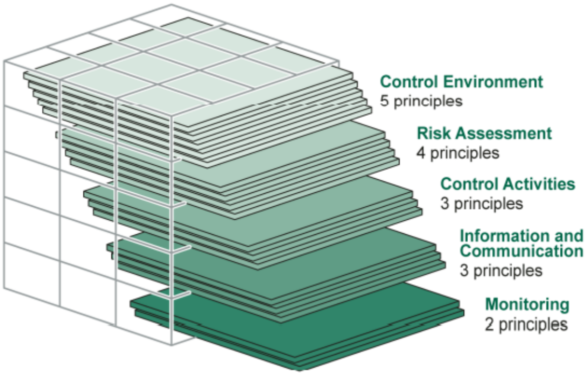
The District's Internal Control Plan aligns with the U.S. Government Accountability Office's (GAO) Standards for Internal Control in the Federal Government (the "Green Book"). The Green Book organizes effective internal control into five integrated components, each of which contains several underlying principles. Together, the five components and 17 principles provide a comprehensive framework for designing, implementing, and operating an effective internal control system across all District activities. And all components and principles are relevant for establishing an effective internal control system. Documentation of the system and its procedures is also required for effective operations and is a critical part of an internal control system.



Sources: COSO and GAO. | GAO-14-704G

This internal control "cube" illustrates the five components of internal control (rows), the three categories of objectives (columns on top), and organizational structure levels (third dimension). An effective internal control system applies all five components to all categories of objectives across the District (entity-wide, divisions, functions, and operating units).

This Internal Control Plan is structured into five parts, one for each component of internal control: Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring. Each chapter explains the component and its relevance to SMCCCD, details the associated principles (17 in total), and provides illustrative examples of key attributes of each principle in a community college district context. The plan is general (it does not rely on specific District data) and is intended for District leaders – including Managers, Directors, Deans, Vice Presidents, college Presidents, Vice Chancellors, the Chancellor, and the Board of Trustees – to guide the establishment and maintenance of effective internal controls District-wide. Implementing this plan will help ensure that the District's three colleges and central services operate ethically, efficiently, and in compliance with applicable requirements, thereby safeguarding public resources and supporting the District's educational mission.



Source: GAO. | GAO-14-704G

PART I: CONTROL ENVIRONMENT

The Control Environment is the foundation of an internal control system – it provides the discipline, structure, and culture that influence the overall quality of internal control. In essence, it is the "tone at the top" set by the Board of Trustees and senior management, which permeates the organization and sets expectations for integrity and accountability. A strong control environment sets a positive tone that encourages ethical behavior, ensures competent leadership, and clearly defines responsibilities throughout the District. According to the Green Book, management and oversight establishes and maintains an environment that demonstrates a commitment to core values and high ethical standards. Part I analyzes the five principles of Control Environment and how SMCCCD can embody them.

PRINCIPLE 1: DEMONSTRATE COMMITMENT TO INTEGRITY AND ETHICAL VALUES

Management and the oversight body demonstrate a commitment to integrity and ethical values. This principle stresses that the Board of Trustees and District leaders set an ethical tone through their directives, attitudes, and behavior. Ethical standards are not merely words on paper – leadership must lead by example in following policies, obeying laws, and treating students, faculty, staff, and the public with honesty and fairness. A strong ethical culture encourages all employees to do what is right, beyond just meeting minimum requirements.

A. **Tone at the Top**: The District's Board of Trustees and executive management (Chancellor and College Presidents) visibly model integrity in all decisions and actions. For example, they communicate openly and truthfully about District matters, honor commitments, and enforce a zero-tolerance stance on fraud or unethical conduct. When leadership consistently behaves ethically, it sends a clear message across all three colleges that ethical conduct is expected of everyone.

B. **Standards of Conduct**: The District currently has established written standards of conduct (e.g. a Code of Ethics or Conduct policy) that define expected ethical behaviors for the Board of Trustees and the District Academic Senate adopted a Statement of Professional Ethics. All District employees are expected to engage in ethical conduct and those expectations are addressed specifically in the larger body of Board Policies and Administrative Procedures (BPs and APs. Examples of topics addressed in BPs and APs include, but are not limited to, conflicts of interest, accepting gifts, and financial integrity).

C. **Adherence to Standards of Conduct**: Management reinforces compliance with a code of conduct by implementing procedures to evaluate and enforce adherence. In practice, this includes requiring annual ethics training and providing safe channels (like a confidential and anonymous hotline) for reporting unethical behavior. If a staff member violates the standards (e.g. misuse of funds or engagement in harassment), the District takes prompt corrective and disciplinary action – such as investigation and appropriate discipline – to demonstrate that unethical behavior is not tolerated. By addressing violations consistently and fairly, management upholds integrity as a core value.

PRINCIPLE 2: EXERCISE OVERSIGHT RESPONSIBILITY

The oversight body oversees the entity's internal control system. In SMCCCD, the oversight body is the Board of Trustees. This principle means the Board actively oversees how internal control is implemented and operates, rather than assuming management alone will handle it. Effective oversight includes providing direction, approving key policies, and monitoring the District's control processes and results.

A. **Oversight Structure**: The Board of Trustees establishes an oversight structure that clearly defines its roles and committees in monitoring internal controls. For example, the Board (or a subcommittee such as an Audit or Finance Committee) could be charged with reviewing internal and external audit reports, following up on identified issues, and assessing the District's risk management efforts. The Board ensures that it receives regular reports from management on the status of internal controls and any significant risks or deficiencies.

B. **Oversight for the Internal Control System**: The Board and top management jointly oversee the design, implementation, and performance of internal controls. In practice, this might involve the Board reviewing and approving an Internal Control Plan (such as this document) and requiring periodic evaluations of controls at each college and the District Office. The Board holds management accountable for resolving control deficiencies – for instance, if an audit finds weak controls over cash handling at a college, the Board expects management to report on corrective measures. Oversight also means asking tough questions: Are financial reports accurate? Are compliance requirements met? Is there any sign of fraud? By staying engaged and inquisitive, the Board provides crucial oversight energy.

C. **Input for Remediation of Deficiencies**: A key part of oversight is ensuring that identified control deficiencies are corrected in a timely manner. The Board fosters an environment where management and staff feel comfortable reporting problems or deficiencies upward (without fear of blame). For example, if college staff discover billing errors or compliance lapses, senior management and the Board are promptly informed. The Board can insist on receiving and reviewing reports of any issues and the plans to fix them. This could include setting up a protocol where significant deficiencies (like material audit findings or compliance violations) are reported to the Board along with management's remediation action plan. By providing input and follow-up on remediation efforts, the oversight body helps ensure continuous improvement of the control system.

PRINCIPLE 3: ESTABLISH STRUCTURE, RESPONSIBILITY, AND AUTHORITY

Management establishes an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives. This principle is about designing the District's organization so that internal control roles and responsibilities are clear. A well-defined organizational structure – including reporting lines and authorization hierarchies – enables the District to carry out its objectives while maintaining accountability at all levels.

A. **Organizational Structure**: SMCCCD's organizational structure is clearly documented and communicated, showing how the District Office and the three Colleges relate to each other. For example, the District's structure might include the Board of Trustees at the top, the Chancellor as chief executive, Vice Chancellors over functional areas (academic affairs, finance, facilities, etc.), and College Presidents leading each campus. Within each college, divisions and departments are delineated. This structure is aligned with the District's objectives – academic, financial, compliance – so that each unit knows its role in achieving those goals. A clear org chart helps everyone understand their place in the control system and avoids gaps or overlaps in responsibility.

B. **Assignment of Responsibility and Delegation of Authority**: Management assigns specific internal control responsibilities to key positions and delegates authority appropriately. For instance, the Vice Chancellor of Finance might be responsible for overseeing financial controls District-wide, while a College President is responsible for controls over campus operations. Authority is delegated such that decisions are made at the proper level: routine expenditure approvals might be delegated to department heads, larger contracts require Vice Chancellor or Board approval, etc. Each person with significant responsibilities (e.g. budget managers, HR directors) is aware of their internal control duties (like reviewing monthly budget reports or approving new hires in accordance with policy). Crucially, delegation is balanced with oversight – those granted authority are accountable to their supervisors and ultimately to the Chancellor/Board for exercising it within policy guidelines.

C. **Documentation of the Internal Control System**: The District documents its internal control system – including its organizational structure, roles, and control processes – in policies and procedure manuals. For example, formal charters describe the authority of the Board committees, administrative procedures outline departmental responsibilities, and an Internal Control Plan (this document) lays out the control framework. Such documentation ensures that as personnel changes occur, the structure and expectations remain clear. It also provides a basis for training staff about their control responsibilities. In a community college setting, this could include documented procedures for everything from student admissions and financial aid processing to procurement and facilities maintenance, each indicating who is responsible for what. Well-documented structure and processes help the District function cohesively and maintain continuity of controls even when staffing or organizational changes happen.

PRINCIPLE 4: DEMONSTRATE COMMITMENT TO COMPETENCE

Management demonstrates a commitment to recruit, develop, and retain competent individuals. Principle 4 highlights that an effective internal control system depends on the people who operate it. The District must have competent personnel at all levels, and management must continually ensure that staff have the knowledge and skills to carry out their responsibilities and adapt to changes.

A. **Expectations of Competence**: The District sets clear expectations for competence in each role, meaning it defines the necessary qualifications and performance standards for personnel. For example, job descriptions for key positions (like accountants, financial aid officers, IT staff, campus security, etc.) specify required education, certifications, and experience. Management's message is that every employee must possess and continue to develop the skills needed to do their job right. Performance evaluations explicitly include an assessment of whether the employee meets competency expectations in areas related to internal control (e.g., understanding of policies, accuracy of work, adherence to procedures).

B. **Recruitment, Development, and Retention of Individuals**: The District employs robust hiring and HR development practices to attract and keep qualified personnel. For instance, when recruiting a new College Business Officer, the District conducts a thorough search to ensure the candidate has strong financial management and compliance skills. Once hired, employees receive training and professional development opportunities (such as workshops on grant compliance, information security, or leadership programs for department chairs) to grow their competencies. The District might implement a mentorship program or tuition reimbursement for staff to obtain relevant certifications (like Certified Public Accountant for accounting staff or IT security certifications for IT staff). Retention is supported by recognizing and rewarding high performance – competent employees are more likely to stay when they feel valued and see a career path. Consistent investment in staff development ensures the District has knowledgeable people to run its controls.

C. **Succession and Contingency Plans**: Management prepares succession plans and contingency arrangements to sustain operations when there are staffing changes or emergencies. For example, the District might cross-train employees in critical functions so that if one person is on leave or resigns, another can temporarily fill their role without major control breakdowns. Key leadership roles (like the Vice Chancellor of Finance or a College President) may have deputies or interim arrangements identified to assume duties if needed. In a community college district, contingency planning could also involve preparing for sudden changes like a pandemic or natural disaster –

ensuring that essential processes (payroll, student registration, etc.) can continue with backup personnel or systems. By proactively planning for transitions and crises, the District demonstrates its commitment to always maintaining competent oversight.

PRINCIPLE 5: ENFORCE ACCOUNTABILITY

Management evaluates performance and holds individuals accountable for their internal control responsibilities. Even with a great culture and competent people, internal control can falter if there is no accountability. This principle focuses on establishing mechanisms to measure and enforce the performance of internal control duties throughout the organization.

A. **Enforcement of Accountability**: The District implements performance measures and incentives that promote accountability for internal control at all levels. Managers and staff are held responsible for complying with internal control policies and achieving control objectives in their areas. For example, a campus financial manager's performance evaluation may include criteria such as timely reconciliation of accounts, adherence to budget limits, and audit results. If a department consistently violates procurement procedures, management addresses it with that department's supervisor, possibly affecting their performance appraisal or eligibility for promotion. Positive accountability is also important – the District can recognize and reward units with exemplary internal control practices (e.g. a "clean" audit). By aligning evaluations, promotions, and recognitions with internal control responsibilities, individuals understand that maintaining control is a core part of their job.

B. **Consideration of Excessive Pressures**: Leadership is mindful of excessive performance pressures that might inadvertently encourage unethical behavior or control overrides. In a college environment, this could mean avoiding unrealistic targets (for instance, overly aggressive enrollment or fundraising goals) that might lead staff to cut corners or misreport results. Management ensures workloads are reasonable and support is provided during peak periods (like registration or year-end closing) so employees are not tempted to bypass controls due to time pressure. For example, if instructors are under pressure to pass a high percentage of students, it might lead to grade inflation or ignoring academic integrity issues – the District mitigates this by balancing expectations and monitoring outcomes. By recognizing and adjusting for undue pressures, the District protects the integrity of processes and prevents situations where staff feel forced to choose between meeting a target and following control procedures.

C. **Accountability in Practice**: The District fosters a culture where everyone understands they are accountable for safeguarding assets, complying with policy, and reporting issues. For instance, budget managers must answer for variances and ensure funds are used appropriately; faculty and staff handling sensitive information (like student records) are accountable for following privacy controls. If a breach or loss occurs, the responsible unit must review what went wrong and strengthen controls. Importantly, accountability is paired with support – when issues arise, the goal is to fix the problem, not to punish unfairly. This encourages honest self-reporting of mistakes. Overall, enforcing accountability means that internal control is taken seriously: people know they will be held to account for doing their part, and this drives a more disciplined and reliable control environment across the District.

SUMMARY OF CONTROL ENVIRONMENT

The Control Environment component establishes the ethical and governance groundwork for all other internal control components. By demonstrating integrity, providing effective oversight, defining clear structures, ensuring staff competence, and enforcing accountability, SMCCCD's leadership creates an environment where internal controls can thrive. A strong control environment is essential — without it, even well-designed procedures may fail, as there would be little incentive for employees to follow them. With the foundation of these first five principles in place, the District is better positioned to identify and manage risks, perform robust control activities, communicate information, and monitor results in the chapters that follow.

PART II: RISK ASSESSMENT

Risk Assessment is the component of internal control that involves identifying and analyzing risks that could prevent the District from achieving its objectives and forming a basis for how those risks are managed. In other words, once SMCCCD has set its objectives (strategic goals, operational targets, compliance requirements, etc.), it must continually ask: "What could go wrong that would keep us from reaching these objectives?" and "How do changes in our environment pose new risks?" By systematically assessing risks, management can prioritize where control activities or other responses are needed. The GAO Green Book states that risk assessment is a dynamic process for identifying risks to defined objectives and evaluating how to address them. This chapter discusses the four principles of Risk Assessment and how the District can apply them.

PRINCIPLE 6: DEFINE OBJECTIVES AND RISK TOLERANCES

Management defines objectives clearly to enable the identification of risks and define risk tolerances. This principle underscores that effective risk assessment starts with clear, specific objectives. If objectives are vague, it will be hard to pinpoint relevant risks. Along with setting objectives, management defines how much risk is acceptable (risk tolerance) in pursuit of those objectives.

A. **Clarity of Objectives**: SMCCCD's leadership clearly defines the District's objectives at various levels – from broad strategic goals down to specific operational targets. For example, an objective might be "Increase student graduation rates by 5% next year" (operational objective), or "Maintain an unrestricted general fund balance of at least 10% of expenditures" (financial objective), or "Comply 100% with state accreditation standards" (compliance objective). Each objective is specific and measurable, providing a basis to identify what risks could threaten its achievement. The District aligns these objectives with its mission and strategic plan and communicates them to all relevant personnel. Clear objectives act as the anchor for risk assessment – everyone knows what success looks like, which makes thinking about risks more concrete.

B. **Definitions of Risk Tolerances**: For each important objective, management defines the risk tolerance – the acceptable level of variation in performance related to that objective. In practical terms, this means deciding how much risk the District is willing to accept. For instance, if the objective is a 5% increase in graduation rates, the District might tolerate a slightly lower increase if it comes with cost constraints, but it might not tolerate any decline in the rate. For financial objectives, risk tolerance could be expressed numerically (e.g. "No more than a 2% budget deficit is acceptable; beyond that level, corrective action is required"). In compliance, risk tolerance might be zero for certain areas (e.g. no tolerance for violating federal financial aid regulations, because the consequences are severe). By defining these tolerances, the District provides guidance on when a risk is within acceptable bounds and when it requires intervention. This helps managers make decisions – for example, if enrollment drops by 1%, that might be within tolerance; if it drops by 10%, it clearly is not and triggers action. Establishing risk tolerances also facilitates more meaningful risk identification, as managers consider not just what could go wrong, but at what point a deviation becomes unacceptable.

PRINCIPLE 7: IDENTIFY, ANALYZE, AND RESPOND TO RISKS

Management identifies, analyzes, and responds to risks related to achieving the defined objectives. This principle describes the core risk assessment process: identifying risks (what could happen), analyzing risks (likelihood and impact), and then deciding on how to respond (what actions to take to address the risk). It is an iterative and ongoing process.

A. **Identification of Risks**: The District proactively identifies risks across all areas of operations, reporting, and compliance. This involves gathering input from various sources – managers at the District Office and colleges, audit findings, community feedback, regulatory changes, etc. Some examples of risks SMCCCD might identify include: a potential drop in state funding, cybersecurity threats to student data, loss of key faculty, natural disasters affecting campus facilities, enrollment fluctuations, changes in federal financial aid rules, or the risk of fraud/theft in cash handling. Each department or function (finance, HR, academic affairs, facilities, etc.) must periodically brainstorm and document the significant risks that could hinder their objectives. The District can use tools like risk assessment workshops or surveys to ensure a comprehensive risk identification. By maintaining a district-wide risk register (a list of identified risks with descriptions), management ensures that everyone is aware of the most significant threats to success.

B. **Analysis of Risks**: Once risks are identified, management analyzes each risk to understand its likelihood of occurring and the potential impact on the District if it does occur. For instance, consider the risk “cyber-attack on student records system.” Management would assess how likely this is (perhaps moderate, given increasing attacks on educational institutions) and how severe the impact would be (very high, due to data loss, privacy breaches, and operational disruption). Risks can be ranked or rated (e.g. using a high/medium/low scale or numerical scores). The analysis might include both qualitative discussion and quantitative data (for example, looking at historical incident frequencies or financial impact estimates). The District also considers how risks interrelate – a risk event in one area (like a budget shortfall) might compound risks in another (like deferred maintenance increasing safety hazards). This analysis helps prioritize which risks need the most urgent attention.

C. **Response to Risks**: Based on the analysis, management decides on risk responses. Common responses include accepting the risk (take no action if it’s within tolerance), avoiding the risk (discontinue the activity causing it), reducing the risk (implement controls or other measures), or sharing the risk (e.g. insurance or outsourcing). In a community college context, many risk responses will involve enhancing internal controls (which is the “reduce” strategy). For example, if analysis shows a high risk of cash theft at campus bookstores, the response might be to strengthen cash handling controls (daily reconciliations, security cameras, dual custody for deposits). If there’s a risk of non-compliance with a new law, the response could be training staff and updating procedures (reducing likelihood). For certain risks, the District might decide avoidance is best – for instance, if a certain program is very costly and risky, the Board might choose not to pursue it. Some risks can be transferred or shared: e.g., purchase insurance for property loss or engage an external service with expertise to manage a complex IT system. The Risk Assessment process must be continuous – as conditions change (new regulations, new technology, etc.), new risks emerge or previously identified ones change in significance, and the District updates its risk responses accordingly. By systematically identifying, analyzing, and responding to risks, SMCCCD management can mitigate threats before they disrupt operations or cause loss.

PRINCIPLE 8: ASSESS FRAUD RISK

Management considers the potential for fraud when identifying, analyzing, and responding to risks. This principle calls for a specific focus on fraud risks – the risk of intentional wrongdoing such as misappropriation of assets, financial reporting fraud, or academic fraud. Public institutions, like a community college district, face fraud risks just as private entities do, and proactive assessment can help prevent or detect fraud.

A. **Types of Fraud**: The District evaluates various types of fraud that could occur within its operations. Common fraud risks in an education context include embezzlement of funds, procurement fraud (kickbacks or fake vendors), theft of equipment or supplies, payroll fraud (ghost employees or overpayments), expense reimbursement fraud, financial aid fraud (students falsifying eligibility or employees manipulating awards), or even academic fraud (such as falsification of student grades or credentials). By considering each area of the District's activities, management enumerates what kinds of fraudulent activities might be possible. For example, in the finance department, a type of fraud could be someone manipulating journal entries to cover a theft; in facilities, it could be misuse of purchase cards or stolen inventory; in student services, it might involve falsifying documents to qualify ineligible students for aid. Recognizing these possibilities is the first step in combating fraud.

B. **Fraud Risk Factors**: Management and the internal audit function (if present) examine fraud risk factors – conditions that could incentivize or enable fraud. The classic fraud triangle factors are: Incentive/Pressure (e.g. financial pressure on an employee, or pressure to meet targets), Opportunity (weak controls that allow fraud to occur undetected), and Rationalization (an attitude or culture that might justify fraud). For instance, if budget cuts create pressure on a department, an employee might feel an incentive to misuse restricted funds for other purposes. Opportunities for fraud could exist if duties are not properly segregated (e.g. one person can both initiate and approve a transaction, or handle cash and reconcile records) or if oversight is lax. The District also considers history (have there been past fraud incidents or complaints?) and areas with high cash flow (bookstores, cafeterias, tuition collection). Additionally, in a college environment, external fraud risk exists (e.g. outside parties attempting phishing scams or false vendor invoicing). By assessing these factors, the District pinpoints where controls may be weakest or pressures highest.

C. **Response to Fraud Risks**: In response to identified fraud risks, the District takes active measures to mitigate them. This includes implementing robust anti-fraud controls such as segregation of duties, regular reconciliations, surprise audits or cash counts, background checks for employees in sensitive roles, and strict oversight of high-risk transactions. For example, to address the risk of payroll fraud, the District's HR and Payroll departments might institute a monthly review of the payroll register against active employee lists and require supervisory approval of timesheets. To mitigate procurement fraud risk, competitive bidding procedures and conflict-of-interest disclosures are enforced for vendors and purchasing staff. The District likely also establishes a confidential reporting mechanism (whistleblower hotline or online report system) so employees, students, or the public can report suspected fraud without fear of retaliation. Reported tips are one of the most common ways fraud is detected, so encouraging a speak-up culture is vital. Furthermore, management develops a fraud response plan – if fraud is suspected or detected, there is a clear protocol for investigation (possibly involving internal audit or external investigators), disciplinary action, and communication to the Board and authorities as appropriate. By anticipating fraud schemes and strengthening preventive and detective controls, SMCCCD significantly reduces the likelihood and impact of fraudulent activities.

PRINCIPLE 9: IDENTIFY, ANALYZE, AND RESPOND TO CHANGE

Management identifies, analyzes, and responds to significant changes that could impact the internal control system. The final Risk Assessment principle emphasizes that the District's internal control system must adapt to change. Changes – whether internal or external – can introduce new risks or alter existing ones, so they must be systematically evaluated and addressed.

A. **Identification of Change**: The District actively monitors for significant changes in its internal and external environment. External changes might include new laws or regulations (for example, changes in California education code, new federal Title IX rules, changes in grant requirements), economic shifts (a recession affecting state funding or student enrollment patterns), technological developments (adoption of a new Student Information System or online learning platform), or societal events (a pandemic, natural disasters). Internal changes could involve organizational restructures (like a new college president or reorganization of departments), new programs or services (launching a new academic program or satellite campus), changes in key processes (centralizing purchasing at the District office), or personnel changes in critical control roles. Management keeps an ear to the ground through industry associations, regulatory updates, strategic planning sessions, and feedback from across the colleges to identify changes early. For example, if the Department of Education announces new financial aid compliance requirements, the change is flagged as a forthcoming risk to compliance objectives.

B. **Analysis of and Response to Change**: Once a change is identified, management analyzes its potential impact on the internal control system and formulates a response. This means asking: How does this change affect our risks and controls? For instance, if SMCCCD implements a new cloud-based financial system, management analyzes whether existing IT controls (user access, data backup, etc.) need updating and whether staff need training to use new control features. If a new regulation requires additional reporting, the District assesses whether current procedures can produce the required data or if new controls are needed to ensure compliance. If enrollment shifts to more online classes, management evaluates whether controls over online learning (like academic integrity, IT security for remote access) are adequate. Responding to change could involve revising policies, redesigning processes, retraining employees, or enhancing monitoring in the transition period. For example, during the COVID-19 pandemic (a significant external change), colleges had to rapidly implement controls for remote operations: electronic approvals replaced physical signatures, new health and safety compliance measures were instituted, and IT controls were strengthened for remote work. SMCCCD would analyze these pandemic-driven changes and adjust its control activities (Chapter 3) accordingly – such as implementing controls for tracking emergency funds usage or updating communication protocols for remote settings. The key is that management treats change as a driver for re-evaluating the control system. The internal control plan is not static; it's updated as needed when the environment changes. By being agile and responsive to change, the District helps ensure that its internal controls remain effective and relevant, thus safeguarding the achievement of objectives even as conditions evolve.

SUMMARY OF RISK ASSESSMENT

Through the Risk Assessment component, SMCCCD management clarifies its objectives, determines acceptable levels of risk, identifies and analyzes risks (including fraud risks), and remains vigilant to changes. This proactive risk mindset allows the District to anticipate problems before they occur and to tailor its control activities (policies and procedures) to areas of greatest risk. In the part we will see how the District's Control Activities are designed and implemented as concrete actions to address the risks identified here. A thorough risk assessment ensures those control activities are properly focused and not just generic controls, thereby making the entire internal control system more effective.

PART III: CONTROL ACTIVITIES

Control Activities are the policies, procedures, techniques, and mechanisms that help ensure management's directives to mitigate risks are carried out . In essence, they are the actions and tools put in place to address the risks identified in Part II, so that objectives can be achieved. Control activities occur throughout the District, at all levels and in all functions, and include things like approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties. According to the GAO Green Book, "Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system". This chapter examines the three principles of Control Activities – covering the design and implementation of control activities, including IT controls – and illustrates key control activities relevant to a community college district.

PRINCIPLE 10: DESIGN CONTROL ACTIVITIES

Management designs control activities to achieve objectives and respond to risks. This principle focuses on thoughtfully designing control activities that directly address the District's risks and objectives. It's not enough to have generic procedures; controls must be tailored to the specific risks (including fraud risks) the District faces, and they ought be deployed at appropriate levels of the organization.

A. **Response to Risks**: SMCCCD designs its control activities as a direct response to the risks identified in the Risk Assessment process. For each significant risk, management determines what control(s) will either prevent the risk from occurring or detect it promptly if it does occur. For example, if the risk is that student tuition revenue might be misstated or lost due to errors or fraud, the District designs controls such as requiring receipts for all payments, reconciling daily cash collections to system records, and independent review of any voided transactions. The objective of accurate financial reporting of tuition is thus met through those specific controls. Importantly, controls are designed with the objective in mind – e.g., to ensure compliance with grant requirements (objective), the District might design a control that every grant expenditure is reviewed for allowability under grant terms before approval (risk of unallowable costs mitigated). By mapping controls to objectives and risks, the District avoids "controls for controls' sake" and instead implements measures that have a clear purpose.

B. **Design of Appropriate Types of Control Activities**: The District uses a mix of control activity types – preventative and detective, manual and automated – as appropriate for the situation . Preventive controls (aimed at stopping errors/fraud before they happen) might include things like requiring approvals before a transaction is executed, access controls in IT systems (so only authorized staff can view or edit records), or physical locks on assets. Detective controls (aimed at identifying issues after the fact) include reconciliations, audits, reviews, and monitoring reports. For instance, a preventive control for payroll might be supervisor approval of timecards, while a detective control is a post-payroll audit report of overtime hours to spot anomalies. Both types are designed to complement each other. The District also balances manual controls (human processes like a manager's review of a report) with automated controls (built into software, like system-enforced validation rules). If SMCCCD's financial system can automatically reject duplicate invoice numbers, that automated control helps prevent double payments. However, the design ensures that even automated controls have human oversight (e.g., someone reviewing exception reports). By employing varied control types, the District creates a robust net of safeguards – some to prevent issues upfront and others to catch what slips through.

C. **Design of Control Activities at Various Levels**: Control activities are designed and deployed at all levels of the District – entity-wide, division, departmental, and functional levels . At the entity-wide level, the Board and executive management may put in place broad controls like policies that apply to all colleges (e.g., a District-wide purchasing policy) or centralized functions (like centralized IT security controls for the entire District network). At the division or college level, controls might be more tailored – for example, each College President's office may institute a review of enrollment and retention data to control for meeting student success objectives. At the department or function level, very specific process controls are in place – the Financial Aid Office has controls for verifying student eligibility, the Maintenance department has a checklist for safety inspections, etc. The design ensures that controls are nested and reinforcing: A department's detailed controls (like verifying a purchase order before payment) support the division's goals (staying within budget), which in turn support entity-wide objectives (financial stability). Additionally, the District considers the interplay between central services and campus-level controls. For instance, if certain payroll functions are centralized at the District Office, the campuses ensure their part (like timesheet submission) feeds into those centralized controls properly. Effective design places controls at the point in the process where they are most effective – sometimes that's on the front lines at a campus department, and other times it's a centralized oversight control at the District level, or both.

D. **Segregation of Duties**: A crucial element of control activity design is segregation of duties, which means dividing tasks among different people to reduce the risk of error or inappropriate actions. The District deliberately structures processes so that no single individual has control over all key aspects of a transaction. For example, in procurement: one person requisitions goods, a different person approves the purchase, another receives the goods, and someone else processes the payment. In accounting, the staff who record journal entries are not the same individuals who reconcile the bank statements. At a campus cashier's office, cash collection, deposit preparation, and deposit verification are split among employees. This segregation ensures that it would take collusion between individuals to perpetrate a fraud, and it increases the likelihood that mistakes are caught by a second pair of eyes. The District periodically reviews job duties and system access rights to ensure adequate segregation is maintained, especially if staffing changes or new systems are introduced. When full segregation is not feasible (for example, in a very small department), the District compensates with other controls, like more frequent supervisory review or rotation of duties. In sum, by carefully designing "who does what," SMCCCD reduces opportunities for errors or fraud to go undetected, thereby strengthening the integrity of its processes.

PRINCIPLE 11: DESIGN ACTIVITIES FOR THE INFORMATION SYSTEM

Management designs the entity's information system and related control activities to achieve objectives and respond to risks. This principle addresses the integration of information technology (IT) and information systems into internal control. The District's information systems (finance system, student information system, HR system, etc.) must be designed or configured with appropriate controls to ensure data reliability, security, and effectiveness in supporting objectives. In modern organizations, many control activities are embedded in IT systems, so careful design of those systems and their controls is essential.

A. **Design of the Entity's Information System**: SMCCCD ensures that its core information systems are designed not just for functionality, but also with internal controls in mind. For example, the District's financial management system (FMS) is set up to enforce the District's approval workflows – the system might require electronic approval from a supervisor before a purchase order is finalized, mirroring the manual control policy. The student information system (SIS) is designed to maintain proper segregation between functions (e.g., a staff member who can update student grades cannot also update tuition balances if not appropriate to their role). When implementing or upgrading any major IT system, the District includes control considerations in the design specifications: such as user access levels, audit trails (the system logs who did what and when), validation checks (the system validates data input, like not allowing an invalid student ID), and error reporting (notifications if something fails, such as a batch process). By embedding controls into the fabric of the information system, many risks (like data entry errors or unauthorized transactions) are mitigated automatically.

B. **Design of Appropriate Types of Control Activities (IT Controls)**: The District distinguishes between general IT controls and application controls, designing both appropriately. General controls are those that apply to the overall IT environment – for instance, controls over data center operations, backup and recovery procedures, system change management, and cybersecurity measures. SMCCCD designs general IT controls such as requiring strong passwords and periodic password changes for all users, using multi-factor authentication for remote system access, regularly backing up critical data and testing disaster recovery plans, and controlling changes to software (ensuring updates are tested before live implementation). Application controls are specific to each software application (finance, HR, student system) – these include things like input controls (e.g., the system prompts for all required fields and checks that inputs are reasonable), processing controls (the system correctly calculates tuition fees or payroll amounts), and output controls (reports are complete and accurate). The District's IT and functional departments collaborate so that application controls align with business process needs. For example, the payroll system might have a gross pay calculation control that flags any paycheck over a certain threshold for review, ensuring anomalies are caught. By designing multiple layers of controls in IT – both at the infrastructure level and within individual applications – SMCCCD helps ensure data integrity and system reliability, which are critical to achieving all objectives (since virtually every objective relies on good information).

C. **Design of Information Technology Infrastructure**: Management also pays attention to IT infrastructure design – the hardware, networks, and software platforms that support the District's systems. A well-controlled infrastructure might include network segmentation (to protect sensitive systems on secure network segments), robust firewalls and intrusion detection systems, secure Wi-Fi configurations on campuses, and up-to-date antivirus and patch management on all servers and workstations. For example, since the District handles sensitive student and employee data, the IT infrastructure is designed to comply with security standards: encrypting data in transit and at rest where appropriate, hosting systems in a secure environment with controlled physical access, and ensuring high availability (so that critical systems like email, online learning platforms, or emergency notification systems have minimal downtime). These infrastructure considerations are part of internal control because a security breach or major IT outage could severely impact operations (risk to objectives). Thus, investing in a solid IT infrastructure with built-in resilience and security controls is a proactive measure to protect the District's ability to function and maintain trust.

D. **Design of Security Management**: A specific aspect of IT controls is security management – controlling who can access what within the District's information systems. SMCCCD designs its user access controls carefully: implementing role-based access where each user's permissions in systems are aligned with their job duties. For instance, a College Admissions clerk might have access to update student contact information but not to modify grades or process tuition refunds; a finance accountant can prepare journal entries but cannot approve their own entries. The District's IT security policies ensure that access is granted only with proper authorization (e.g. supervisors must approve new accounts or permission changes) and that access rights are reviewed periodically to revoke any that are no longer needed (such as when an employee transfers or leaves). Multi-factor authentication and session timeouts might be employed for particularly sensitive systems (like those containing personal identifiable information or financial data). Additionally, security management involves monitoring for potential intrusions or unauthorized activities – for example, logs of failed login attempts might be reviewed, or software alerts set to detect unusual data downloads. By designing strong security controls, the District reduces the risk of data breaches, data tampering, or other security incidents that could compromise its objectives or lead to compliance violations (such as FERPA or HIPAA breaches in student or health records).

E. **Design of IT Acquisition, Development, and Maintenance**: Finally, SMCCCD integrates controls into the process of acquiring or developing new IT systems and maintaining existing ones. When the District considers purchasing a new software system (say, a curriculum management system), part of the selection criteria is the system's ability to meet internal control requirements (e.g., does it have audit trail functionality? Can it enforce approval workflows?). During development or implementation, the District follows change management controls: requirements are documented, changes are tested in a staging environment, and data conversion is verified for accuracy. For in-house developed reports or tools (for instance, a custom enrollment reporting tool), there is peer review of the code or logic to ensure accuracy. Maintenance of systems (applying patches, upgrading versions) is done in a controlled manner – IT schedules downtime, informs users, tests the updates, and has a rollback plan if something goes wrong. By embedding such controls in the IT lifecycle, the District avoids introducing new vulnerabilities or errors when systems change. In short, the design of control activities for information systems covers everything from daily automated checks to the governance of big IT projects, ensuring technology fully supports, rather than undermines, the internal control framework.

PRINCIPLE 12: IMPLEMENT CONTROL ACTIVITIES

Management implements control activities through policies (that establish what is expected by the Board of Trustees) and procedures (that put policies into operational action). Designing controls is crucial, but they only work if properly implemented and executed. This principle is about putting the designed control activities into operation throughout the District – effectively deploying policies and procedures and ensuring they are followed consistently.

A. **Documentation of Responsibilities through Policies**: SMCCCD formally documents its control activities in policies and procedures so that personnel have clear guidance on their responsibilities. For example, the District might have an Administrative Procedures Manual or a series of Board Policies that cover key processes: e.g., a procurement policy describing required approvals and bid procedures, a travel policy outlining allowable expenses and required receipts, a student records policy specifying who can update student data, etc. Each policy communicates the control objectives and the required activities to achieve them. Alongside policies, detailed procedures or work instructions are developed at the department level – for instance, the Accounts Payable procedure will detail how an invoice is logged, matched to a purchase order, approved, and paid, including which documents to review and who signs off. These documents assign responsibility (who does each task) and describe the timing/frequency of the control (e.g., bank reconciliations must be completed within 30 days of month-end). By codifying control activities in writing, the District ensures that expectations are not just passed along verbally (which can lead to inconsistency or forgetfulness). New and existing employees alike can refer to these written policies to understand how to perform their duties in compliance with internal controls. Moreover, having documentation is itself a control – it enables monitoring (Chapter 5) because you can check actual practices against the written procedures.

B. **Periodic Review of Control Activities**: Management establishes a process for regularly reviewing and updating policies and procedures to keep control activities effective and relevant. Over time, processes change (as discussed in Principle 9), or a control may prove inefficient or insufficient. The

District schedules periodic policy reviews (say, annually or biennially) where key stakeholders and possibly internal auditors examine whether procedures are being followed and if they need refinement. For example, if a policy is found to be routinely bypassed or causing bottlenecks (perhaps a certain approval takes too long and delays operations), management analyzes why – maybe the policy needs adjustment or better enforcement. Likewise, if new regulations come out, related control policies are updated promptly. The District might maintain a compliance calendar to ensure all critical control policies (finance, IT, HR, etc.) are reviewed on a set cycle. In implementing control activities, training is also part of the process: the District trains employees on new or updated procedures and reinforces existing controls through refreshers. For instance, each fiscal year, budget managers might get a brief training on any changes in financial procedures or reminders about adhering to budget controls. Automating reminders is another technique – e.g., the system could send an alert if a monthly reconciliation is overdue, prompting staff to complete it. By monitoring the implementation and maintenance of control activities, the District avoids "policy drift" (where practice diverges from written policy over time) and keeps controls operating as intended.

C. **Consistent Implementation Across the District**: With three colleges and central services, SMCCCD strives for consistency in implementing controls while allowing for necessary local adjustments. This means that if a policy applies District-wide (like payroll or accounting procedures), each college follows the same fundamental steps so that controls are uniformly strong. Management communicates expectations clearly across all campuses – perhaps via District-wide administrative directives or regular meetings of college administrative VPs – to ensure no campus is a weak link. At the same time, the District acknowledges differences in operations; for example, a smaller campus might have fewer staff, so they implement a segregation of duties control in a slightly different way (with one person wearing two hats but a compensating review by a District Office official). The key is that the spirit of the control is met everywhere. The District may use internal audits that sample each college to verify that procedures are implemented properly and consistently. If one college has found an innovative way to strengthen a control (say, an electronic checklist for lab safety inspections), the District can share that best practice so others can implement it too. Ultimately, implementing control activities is about going from paper to practice – ensuring that every day, in hundreds of transactions and decisions across the District, the prescribed controls are actually being performed. Through strong policies, training, oversight, and continuous improvement, SMCCCD turns its control designs into real actions that safeguard its operations.

SUMMARY OF CONTROL ACTIVITIES

The Control Activities component is the hands-on part of internal control – it is where policies and procedures are executed to prevent or detect issues. SMCCCD designs a robust portfolio of control activities (including proper segregation of duties and IT controls) and implements them via clear policies and diligent procedures. By doing so, the District ensures that the risks identified in Part II are being managed daily. Examples cited – like approvals, reconciliations, access controls, and physical safeguards – are all in service of keeping the District on track toward its objectives. In the next component, we address how information flows and communications enable these control activities and the overall system to function effectively.

PART IV: INFORMATION AND COMMUNICATION

No control system can succeed without information and communication. This component is about ensuring the District obtains relevant, timely, and quality information and then effectively communicates that information to those who need to know, internally and externally. Information is the raw material of decision-making and control – it includes data about operations, financial results, compliance status, etc. Communication is the process of sharing that information in the right form and time so that personnel can carry out their responsibilities and external stakeholders can be informed. The GAO Green Book highlights that "management uses quality information to support the internal control system" and that "effective information and communication are vital for an entity to achieve its objectives". In a multi-campus district, strong communication channels – both vertical (up and down the chain of command) and horizontal (across departments and campuses) – are essential to coordinate internal control efforts. This chapter covers the three principles of Information and Communication.

PRINCIPLE 13: USE QUALITY INFORMATION

Management uses quality information to achieve the entity's objectives. This principle emphasizes that the District must identify its information needs and ensure the information used for internal control is appropriate – meaning it is timely, current, accurate, and accessible. "Quality information" is the fuel that enables the District to make informed decisions, monitor performance, and detect issues.

A. Identification of Information Requirements: SMCCCD management determines what information is needed at various levels to run the District and monitor internal controls. This involves mapping out information requirements for each objective and each key decision-maker. For example, to manage the objective of fiscal health, the Chancellor and Board need monthly financial reports that include budget-to-actual comparisons for each college and major fund. Department managers might need weekly or daily operational reports (like enrollment numbers, course fill rates, or maintenance work order backlogs) to manage their specific areas. Compliance officers need information on regulatory deadlines and status of compliance activities (e.g., status of Clery Act reporting, or status of audit findings remediation). By clearly identifying these needs, the District can design its information systems and reporting processes to produce the right data. Often, this results in developing dashboards or summary reports for high-level monitoring and detailed reports for transactional review. Importantly, information requirements also include data from external sources when relevant – for instance, benchmarks from other community colleges, economic indicators for enrollment forecasting, or updates from the state chancellor's office. Recognizing all these requirements ensures that internal control is supported by a comprehensive information set.

B. **Relevant Data from Reliable Sources**: Once information needs are known, the District gathers relevant data from reliable sources . Relevance means the data has a logical connection to the control or decision at hand. If a risk being monitored is student absenteeism (impacting student success objectives), relevant data would be attendance records and dropout rates, rather than, say, unrelated data like parking permit sales. Reliability means the data is accurate, complete, and obtained from a trustworthy process. SMCCCD invests in information systems (or manual processes, where needed) that produce reliable data – for instance, ensuring that the student attendance tracking system is used consistently by instructors so that the data is complete, or that financial data is reconciled and reviewed for accuracy. The District might use automation to reduce manual errors (like direct data feeds from one system to another rather than re-keying information). Additionally, data validation checks (a kind of control activity) help maintain data quality – e.g., input controls in systems ensure dates or dollar amounts fall in expected ranges. When using external data, the District considers its source: for example, a state economic forecast would be considered a reliable source for projecting local property tax revenue, whereas an unverified source on the internet would not. By focusing on relevant and reliable data, management can trust the information when analyzing performance or identifying issues.

C. **Data Processed into Quality Information**: Having raw data is not enough; the District must process and analyze data to convert it into useful information. This means summarizing, contextualizing, and communicating data in a way that stakeholders can understand and act on. For example, the District's Finance team might take thousands of lines of transaction data and process them into a concise financial report with key indicators, variance analyses, and charts that highlight trends. Context is provided by comparing data to benchmarks or expectations (such as current enrollment vs. last year's enrollment, or expenditure vs. budget). The IT department may assist by providing reporting tools or business intelligence systems to generate these analyses routinely. Quality information is characterized by its clarity and usefulness – for instance, a report that flags departments exceeding budget by more than 5% provides a clear call to action. Similarly, an incident report that categorizes types of IT security breaches helps management see patterns and respond accordingly. In processing information, timeliness is crucial: information arrives with enough speed that decisions can be made (e.g., weekly enrollment updates during registration periods so adjustments can be made to course offerings if needed). The District avoids information overload by focusing reports on key metrics and exceptions, rather than drowning managers in unnecessary details. By refining raw data into actionable insights, SMCCCD's management enables effective internal control decisions and adjustments. For example, if processed information shows a downward trend in a particular college's attendance, management can investigate and respond (perhaps by increasing student engagement efforts) well before it becomes a critical problem. In summary, quality information is fit for purpose – it meets the needs identified, comes from reliable data, and is processed into a form that supports sound management and control.

PRINCIPLE 14: COMMUNICATE INTERNALLY

Management internally communicates the necessary quality information to achieve the entity's objectives. This principle is about the internal flow of information – up, down, and across the organization. To keep the internal control system working, the right people must get the right information at the right time. Internal communication encompasses formal and informal channels: reports, meetings, emails, hotlines, and face-to-face conversations that ensure everyone understands their duties and can report on their activities.

A. **Communication throughout the Entity**: SMCCCD fosters open two-way communication across all levels – from the Board and Chancellor's Office to college administration to faculty and staff on the ground. Management communicates downward by disseminating policies, plans, and expectations. For example, after the Board approves an updated internal control policy or the annual budget, that information is communicated to campus administrators via memos and meetings, who then pass relevant instructions to department heads and employees. Conversely, upward communication is encouraged so that frontline personnel can raise concerns or provide feedback. If a cashier in a college business office notices a flaw in a procedure or suspects a control issue (like frequent discrepancies in cash counts), there must be a clear path to communicate this to higher management without fear. This could be done through supervisory channels or more directly through an internal hotline or suggestion program. Lateral communication is also important: departments share information with each other as needed (for instance, the Financial Aid office communicating with the Finance office about a reconciliations issue, or IT communicating with all departments about a security alert). The District may establish cross-functional committees or working groups (e.g., a Risk Management Committee or Compliance Committee) that bring together representatives from various campuses and functions to share information on internal control matters, risks, and best practices. By facilitating widespread communication, the District ensures that information doesn't stay siloed – everyone knows what they need to know to do their part in the control system.

B. **Appropriate Methods of Communication**: Management uses varied methods of internal communication suited to the audience and importance of the message. Formal communications include written policies and procedures (available perhaps on a District intranet or policy portal) so employees can reference authoritative guidance at any time. Regular staff meetings at all levels (Board meetings, Chancellor's cabinet meetings, College leadership meetings, departmental meetings) are a platform to communicate priorities, report on performance, and discuss control issues. Email bulletins or newsletters might be used to highlight key updates (e.g., end-of-fiscal-year procedures, or reminders about safety protocols). For critical or sensitive matters – such as an emerging fraud concern or a serious compliance violation – management may communicate through special briefings or secure channels to the relevant personnel. Additionally, training sessions are a form of communication: for example, an internal controls training provided to all department heads communicates both the importance of controls and the specifics of what is expected. The District ensures that communications are clear and accessible: using plain language (avoiding unnecessary jargon), translating or providing interpretation if needed for employees with language barriers, and using diagrams or charts for complex processes. It also ensures timeliness – an important announcement (like changes in emergency procedures) is communicated promptly via multiple channels (email, text alert, posted on bulletin boards). Finally, the District gauges the effectiveness of its communication methods by seeking feedback. For instance, a quick survey might be sent after a policy update to see if recipients understood the message. By using appropriate methods – from high-tech solutions like an intranet dashboard to simple in-person meetings – SMCCCD maximizes the chance that vital information reaches everyone who needs it, and that people feel informed and heard within the organization.

C. **Embedding Communication in the Culture**: Internal communication for control purposes is not just about memos and meetings – it's part of the District's culture. Management tries to create an environment where employees at all levels feel comfortable communicating about problems or improvements related to internal controls. For example, if a faculty member spots a discrepancy in a grant expense report, they know how to report it and trust that management will address it constructively. The District might have an open-door policy or designated ombudspersons for staff to approach with concerns. Moreover, successes are communicated too – when a campus or department demonstrates exemplary internal control (like a clean audit or successful implementation of a new system), management shares that news, which reinforces positive behaviors and knowledge transfer. By making internal communication a continuous, multi-directional process, SMCCCD ensures that information flows effectively as the lifeblood of its internal control system.

PRINCIPLE 15: COMMUNICATE EXTERNALLY

Management externally communicates the necessary quality information to achieve the entity's objectives. This principle covers communication with external parties – stakeholders outside the District's internal chain of command. External communication is key for transparency, accountability, and obtaining outside information that can impact the internal control system. Stakeholders include oversight agencies, auditors, students and their families, local community, creditors, granting agencies, and others. The District needs to both send information out and receive relevant feedback or guidance from external sources.

A. **Communication with External Parties**: SMCCCD provides relevant and timely information to external stakeholders such as regulators, funding bodies, and the public . For example, the District prepares an Annual Financial Report for the public and bondholders, disclosing its financial condition in accordance with Government Accounting Standards – this is an external communication that demonstrates financial accountability. The District also submits required reports to state and federal agencies (such as enrollment reports to the state chancellor's office, compliance reports for federal grants, or data for accreditation reviews). Management ensures these communications are accurate and complete – which is an outcome of the internal control system producing reliable information (Principle 13) and review processes to catch errors before submission. Additionally, the District communicates relevant internal control information to its external auditors. During the annual independent audit, District management is expected to be candid and transparent about controls, known issues, and actions taken; this might involve management letters, representations, and providing documentation. External communication also involves the District listening to outside feedback: student and community input (perhaps through surveys or public comment at Board meetings) can highlight issues like service quality or safety concerns that management could incorporate into its risk assessment and controls. For example, if community members signal concerns about campus security, the District will treat that as important information and possibly respond by enhancing related controls or procedures (like improving campus lighting or increasing patrol presence). Thus, communication is two-way – the District not only reports out but also actively solicits and receives information from outside that can help improve internal operations.

B. **Appropriate Methods of Communication**: The District uses appropriate channels and formats to communicate externally, depending on the audience and purpose. Formal communications include official reports, press releases, the District's website postings, and required public filings. For instance, financial statements are published on the District's website and perhaps presented in a public Board meeting, allowing citizens and oversight bodies to review them. When communicating compliance information, the District may prepare standardized templates or forms required by agencies (like the IPEDS report for federal education statistics or the annual Clery Act campus crime statistics report). For urgent or significant issues – such as a data breach or a major audit finding – the District would likely issue a formal notification or press statement to ensure transparency. On the other hand, routine communications with external parties might be handled through established liaisons: e.g., a designated Grant Manager communicates with grant program officers about project status and any compliance questions; the internal auditor or finance director communicates with the external auditors regularly throughout the year, not just at audit time. The District also leverages technology for external communication: it might maintain an online portal where vendors can see procurement opportunities and related internal control requirements (like conflict-of-interest policies), or a student portal where students receive notices about financial aid requirements or policy changes affecting them. Social media and community newsletters can be used to share successes (like clean audit results or improvements in services) with the broader community, demonstrating the District's commitment to accountability. In choosing communication methods, the District considers clarity and audience understanding – for example, financial information might be summarized in layperson's terms for the general public, whereas detailed technical data is provided to regulators and experts. By tailoring its external communications appropriately, SMCCCD maintains trust and meets its accountability obligations, while also keeping lines open for valuable external input.

SUMMARY OF INFORMATION AND COMMUNICATION

In summary, SMCCCD's internal control system is supported by a strong Information and Communication component. Quality information is identified, collected, and processed to support all other control functions. That information is then communicated internally so that every employee knows what they need to do and can alert management to issues and communicated externally to stakeholders and oversight bodies to maintain transparency and gather outside perspectives. By treating information as an asset and communication as a priority, the District enables informed decision-making and swift corrective actions, reinforcing all components from Control Environment through Monitoring. Communication truly links all parts of the framework: a value promoted by the tone at the top, necessary for identifying risks, essential for executing control activities, and fundamental for effective monitoring (as we will see next).

PART V: MONITORING

Even a well-designed internal control system needs to be monitored to ensure it continues to operate effectively. Monitoring is the component that involves ongoing and periodic evaluations of the internal control system and taking action on any deficiencies found. The GAO Green Book describes internal control monitoring as a dynamic process where internal control is assessed over time and modified as needed. Monitoring gives the District feedback – it answers the question, "Are our controls working as intended, and if not, what are we doing about it?" This chapter covers the two principles of Monitoring: performing monitoring activities and evaluating and addressing deficiencies. Effective monitoring at SMCCCD means the District doesn't set and forget its internal controls – it continually watches over them and improves them.

PRINCIPLE 16: PERFORM MONITORING ACTIVITIES

Management establishes and operates monitoring activities to monitor the internal control system and evaluate the results. This principle directs the District to implement both ongoing monitoring (built-in, continuous checks) and separate evaluations (periodic assessments by objective parties) of its internal controls. By doing so, management can promptly identify when controls are not functioning optimally or when circumstances have changed.

A. **Establishment of a Baseline**: As a starting point for monitoring, SMCCCD management establishes a baseline of internal control effectiveness. This baseline might be set through an initial comprehensive evaluation of controls – for example, an internal control self-assessment or an internal audit that documents the current state of controls and any known deficiencies. The baseline represents the standard against which future performance is compared. For instance, management might document at Year 1 that bank reconciliations are completed within 30 days 90% of the time (baseline measure) or that currently 100% of employees have completed ethics training. With this baseline, if performance slips (say, timely reconciliations drop to 70% in a later period), monitoring will catch that deviation. Establishing a baseline could also involve reviewing past audit results and management evaluations to know where key risk areas are and what "normal" looks like. In effect, the baseline is a snapshot of the control system's design and operation at a point in time, which will be used as a reference for ongoing monitoring efforts.

B. **Internal Control System Monitoring (Ongoing Monitoring)**: The District conducts ongoing monitoring of controls as part of regular operations. Ongoing monitoring means that managers and staff who perform control procedures also routinely check whether the procedures are working. It is often integrated into the day-to-day supervision. For example, a department supervisor might spot-check transactions every week, or the payroll manager might review an exception report each pay period as part of their normal duties – these are monitoring actions embedded in operations. College business offices might use monthly checklists to review key controls (like verifying all account reconciliations were done or confirming that all new vendors went through approval). Information systems can automate some ongoing monitoring: e.g., generating an alert if a certain control threshold is breached (like budget expenditure exceeds authorized limits). Ongoing monitoring also includes regular supervisory activities like observing employees' adherence to procedures, asking questions when something looks off, and rotating duties temporarily to get a fresh look at a process. The District's culture (from the Control Environment) plays a role here – if managers value internal control, they naturally include these checks in their routine. SMCCCD likely uses internal dashboards or metrics to monitor controls in real-time: for instance, tracking the number of overdue audit issues or the percentage of training compliance. Because ongoing monitoring is continual, it can lead to early detection of anomalies. If, say, a certain expense account starts showing unusual activity mid-year, the continuous review by the finance team can trigger an immediate inquiry rather than waiting for year-end. Essentially, ongoing monitoring is the "eyes on the process" every day that helps ensure controls are present and functioning.

C. **Separate Evaluations**: In addition to ongoing monitoring, SMCCCD performs separate evaluations of internal control – these are more periodic and often more formal assessments, which may be done by people not involved in the daily operations of the controls. Separate evaluations can include internal audits, external audits, or special reviews. For instance, the District's Internal Audit (or an external consultant if internal audit is small) might annually review a particular area such as procurement or IT security, testing whether controls are adequate and effective. The Board's Audit Committee might commission an enterprise-wide internal control review every few years. Additionally, the District could engage in peer reviews with other districts or ask managers from one campus to review processes at another – bringing a fresh, independent perspective (this cross-campus review could be a creative way to simulate an independent evaluation). Separate evaluations are planned and scoped to cover all major control areas over time. They are valuable because ongoing monitoring by itself might miss systemic issues – people can become accustomed to the way things are, whereas an independent look can identify problems or improvement opportunities. For example, an internal audit might discover that while managers are checking reconciliations, they haven't noticed a pattern of small errors that indicate a training issue, whereas the auditor's broader sampling reveals it. SMCCCD schedules these evaluations based on risk – high-risk areas (like financial reporting, large grant programs, or IT security) are reviewed more frequently, while lower-risk areas less so. The results of separate evaluations are reported to senior management and the Board, providing an objective view of how well the internal control system is working overall.

D. **Evaluation of Results**: Both ongoing monitoring and separate evaluations produce findings – data and observations about control performance. Management evaluates these results to determine if the internal control system is effective or if deficiencies exist. For example, the District compiles the results of monthly control checklists (ongoing monitoring) and notes if any control tasks were skipped or problematic. Or, when an internal audit report is issued (separate evaluation), management reviews the significance of any findings. Evaluation involves discerning patterns: Is a particular control failing repeatedly? Are certain departments consistently struggling with compliance? Are we seeing improvement or deterioration in key control metrics over time? If the evaluation finds that controls are not performing as intended – perhaps a spike in errors or an uptick in incidents of non-compliance – management considers whether the design of controls is flawed or if implementation is lacking. Sometimes the evaluation might conclude the system is effective in design but needs stronger enforcement, or vice versa. A part of evaluation is updating the internal control baseline – essentially resetting the benchmark after improvements or changes have been made, so the next round of monitoring has a new point of reference. The outcome of this evaluation step is a decision on whether any issues warrant reporting and remediation, leading into Principle 17. In summary, through systematic monitoring activities, SMCCCD continually takes the pulse of its internal controls. This proactive approach ensures that control deficiencies are not allowed to fester; instead, they are caught and addressed early, keeping the system healthy and reliable.

PRINCIPLE 17: EVALUATE ISSUES AND REMEDIATE DEFICIENCIES

Management remediates identified internal control deficiencies on a timely basis. This final principle completes the feedback loop of internal control. When monitoring (Principle 16) or other sources (like external audits or employee reports) uncover problems or weaknesses in controls, the District must take prompt action to address them. It's not enough to find issues – they must be reported to the right people, evaluated for significance, and corrective actions must be implemented. This ensures continuous improvement of the internal control system.

A. **Reporting of Issues**: SMCCCD has mechanisms for reporting internal control issues to appropriate levels of management and the Board so that deficiencies are recognized and tracked . For instance, if a department head discovers a compliance violation (say, procurement procedures not being followed in a particular instance), they report it through the chain of command – possibly to the College President and the central administration. Significant issues, such as a material weakness in financial controls or a suspected fraud, would be escalated to senior leadership and the Board's Audit Committee immediately. The District likely maintains an issue log or audit finding tracking system. Internal Audit or another designated officer might compile all identified control issues (from audits, monitoring, hotline complaints, etc.) in one place and regularly update management on their status. In addition to formal channels, the District encourages a culture where employees can freely bring up control concerns (related to Principle 14's internal communication). For example, if a staff member notices that password sharing is common in their office (a security control violation), hopefully they feel empowered to report that issue, perhaps anonymously via a hotline if needed. SMCCCD ensures that reports of issues are documented and include details so they can be evaluated – what exactly happened, what control failed, what the potential impact is, etc. This documentation is important when later assessing the severity and deciding on actions.

B. **Evaluation of Issues**: Once an issue is identified and reported, management evaluates the issue to determine its significance and the root cause. Evaluation might involve asking questions like: Is this an isolated incident or a systemic problem? Does it indicate a flaw in control design or was it a failure in execution (compliance)? What is the impact – financial loss, legal exposure, operational disruption, reputational damage? For example, an identified deficiency might be that a particular bank reconciliation was not done for two months. Management would evaluate: was this due to staff turnover (and thus a one-time lapse) or due to a broader issue like inadequate staffing or unclear responsibility (a systemic issue)? And did it result in any undetected errors or fraud in the account? The District classifies deficiencies into categories such as control deficiency, significant deficiency, or material weakness (terms often used in auditing) based on their severity. A minor control deficiency (like a small training gap) might be handled at the department level, whereas a material weakness (e.g., revenues being recorded without proper review, leading to misstatements) would be reported to the highest levels and perhaps disclosed externally. In evaluation, root cause analysis is key: management doesn't just treat the symptom but digs into why the deficiency occurred. For instance, if multiple colleges had procurement violations, maybe the procurement policy is overly complicated or not well communicated – the root cause might be policy design or training rather than deliberate disregard by staff. Understanding the cause guides the remediation.

C. **Corrective Actions**: Finally, SMCCCD management implements corrective actions to remediate deficiencies and tracks their completion. Corrective action plans are developed for each significant issue. These plans assign responsibility (who will fix it), describe what will be done (e.g., update a procedure, provide training, increase supervision, add a control step, or in some cases discipline personnel), and set a timeline for completion. For example, if an audit finds that access to the network server room was not adequately restricted, a corrective action could be installing an electronic card key system and updating the access list within 3 months, with the Director of IT responsible. The District's leadership monitors the progress of these action plans in management meetings or through status reports. It's important that once fixes are implemented, they are tested to confirm the deficiency is resolved – essentially a follow-up evaluation. In some cases, a quick fix is possible; in others, it may take time (for instance, addressing a material weakness in financial reporting might involve replacing an outdated system, which could take a year – interim measures would be put in place meanwhile). The Board or Audit Committee often oversees major remediation efforts, especially if they were the ones to whom the issue was reported initially. They will expect updates and ultimately a report that the issue has been addressed. Moreover, the District integrates lessons learned from each issue back into the system: policies might be revised to prevent recurrence, training programs adjusted to cover the gap, or monitoring enhanced in that area going forward. By diligently following through on corrective actions, SMCCCD closes the loop – ensuring that identified problems lead to tangible improvements. This continuous improvement cycle helps the internal control system evolve and strengthen over time, even as new challenges arise.

SUMMARY OF MONITORING

The Monitoring component ensures that SMCCCD's internal controls are not static but are continuously assessed and improved. Through ongoing monitoring embedded in daily operations and separate evaluations by independent parties, the District gains visibility into the effectiveness of its controls. When issues are found, the District's internal communication channels (from Principle 14) and accountability structures (from Principle 5) kick in to ensure those issues are reported, evaluated, and fixed. This proactive monitoring and remediation process means that small problems are addressed before they become large failures, and the internal control system remains dynamic and responsive to new risks and changes. In essence, monitoring is like the District's immune system – detecting and responding to control weaknesses to keep the organization healthy and able to achieve its academic and operational mission.

CONCLUSION

In conclusion, the San Mateo County Community College District's Internal Control Plan – structured around the five components and 17 principles of the GAO Green Book – provides a comprehensive framework for responsible governance and management across all three campuses and central services. By nurturing a strong Control Environment (ethical tone, oversight, structure, competence, and accountability), rigorously conducting Risk Assessment (clear objectives, risk identification including fraud, and adapting to change), implementing targeted Control Activities (well-designed policies, procedures, and IT controls, executed with discipline and documentation), maintaining robust Information and Communication (ensuring quality information flows to those who need it internally and externally), and performing continuous Monitoring (ongoing reviews and prompt remediation of deficiencies), District leadership can have reasonable assurance that its objectives will be achieved in an effective and compliant manner .

This Internal Control Plan is intended to be a living and aspirational document. District management and the Board of Trustees reviews and updates the plan periodically to reflect new strategic goals, emerging risks, and lessons learned from monitoring and audits. Ultimately, internal control is a means to an end – helping SMCCCD fulfill its mission of educating students and serving the community with integrity, efficiency, and excellence. By following this plan and modeling the Green Book standards, District leadership will speak a common language of internal control, make informed decisions, and collectively safeguard the District's resources and reputation. Through steadfast commitment to these principles, SMCCCD will strengthen public trust and ensure that it continues to provide high-quality education in a well-controlled and accountable environment for years to come.